TI - System for detecting back door of kernel, and method for detecting back door of kernel and recovering data of kernel

PR - KR20020024844 20020506
PN - KR2003086722 A 20031112 DW200420 G06F11/00 001pp
PA - (ELTE-N) ELECTRONICS & TELECOM RES INST
IC - G06F11/00
IN - KIM H C

AB - KR2003086722 NOVELTY - A kernel back door detection system and method, and a kernel data recovering method are provided to detect a vicious kernel back door like a Linux kernel back door, and to recover the data, changed by the vicious kernel back door, into normal data.
- DETAILED DESCRIPTION - The system comprises a kernel module manager(110), an allowance kernel module manager(210), an allowance kernel module database(220), and a kernel module loading manager(230). The kernel module manager(110), positioned at a user area, embeds a kernel module management program for adding, deleting or searching a list of an allowance kernel module. The allowance kernel module manager(210) manages the list of the allowance kernel module which the kernel module manager requests to be registered. The allowance kernel module database(220) stores the list of the allowance kernel module allowed to be registered by the allowance kernel module manager(110). The kernel module manager(230) loads the kernel modules, which the user area requests to be loaded, at a kernel area based on the list of the allowance kernel module.
- (Dwg.1/10)

OPD - 2002-05-06
AN - 2004-211180 [20]

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
G06F 11/00

(11) 공개번호 특2003-0086722
(43) 공개일자 2003년11월12일

(21) 출원번호 10-2002-0024844
(22) 출원일자 2002년05월06일

(71) 출원인 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 김흥철
대구광역시북구침산3동동아무지개아파트203동801호

(74) 대리인 신영무

심사청구 : 있음

(54) 커널 백도어 탐지 시스템, 이를 이용한 커널 백도어 탐지방법 및 커널 데이터 복구 방법

요약

본 발명은 리눅스 커널 백도어 탐지 시스템, 이를 이용한 커널 백도어 탐지 방법 및 커널 데이터 복구 방법에 관한 것으로, 리눅스 커널 백도어와 같은 악성 커널 모듈을 탐지할 수 있는 커널 백도어 탐지 시스템 및 탐지 방법을 제공하고, 리눅스 커널 백도어에 의해 변경된 커널 데이터를 정상적인 상태로 복구 시킬 수 있는 커널 데이터 복구 방법을 제공하는데 그 목적이 있다.

이를 위해, 본 발명에서는 커널 공간의 메모리 영역에 적재가 시도되는 리눅스 커널 모듈에 대해서 1차적으로 그 모듈이 적재가 허용되는지를 검사하는 1차 커널 백도어 탐지 과정과, 2차적으로 메모리 영역에 적재되는 커널 모듈이 커널 백도어와 같은 악성 커널 모듈로서 커널 데이터를 변경시키는지를 탐지하는 2차 커널 백도어 탐지 과정과, 변경된 커널 데이터를 다시 정상적인 값으로 복구시키는 복구 과정을 제공한다.

따라서, 본 발명은 리눅스 시스템 내에 커널 백도어와 같은 악성 커널 모듈이 설치되는 것을 효과적으로 탐지하고, 커널 백도어에 의해 변경된 커널 데이터를 정상적인 커널 데이터로 복구시킬 수 있는 효과가 있다.

대표도

도 1

색인어

리눅스, 커널 백도어, 커널 모듈, 커널 데이터, 보안 커널 모듈 목록

명세서

도면의 간단한 설명

도 1은 본 발명의 바람직한 실시예에 따른 리눅스 커널 백도어 탐지 시스템의 구성도이다.

도 2는 도 1에 도시된 리눅스 커널 백도어 탐지 시스템의 동작 과정중 '등록 과정'을 설명하기 위해 도시한 흐름도이

다.

도 3은 도 1에 도시된 리눅스 커널 백도어 탐지 시스템의 동작 과정중 '1차 커널 백도어 탐지 과정'을 설명하기 위해 도시한 흐름도이다.

도 4는 도 1에 도시된 리눅스 커널 백도어 탐지 시스템의 동작 과정중 '2차 커널 백도어 탐지 과정'을 설명하기 위해 도시한 흐름도이다.

도 5는 도 1에 도시된 리눅스 커널 백도어 탐지 시스템의 동작 과정중 '복구 과정'을 설명하기 위해 도시한 흐름도이다.

〈도면의 주요 부분에 대한 부호의 설명〉

100 : 사용자 공간 200 : 커널 공간

110 : 커널 모듈 관리부 120 : 적재 커널 입력부

210 : 허용 커널 모듈 관리부 220 : 허용 커널 모듈 데이터베이스

230 : 커널 모듈 적재 관리부 240 : 커널 데이터 검증/복구 모듈부

250 : 커널 원본 데이터베이스 260 : 시스템 콜 감시/복구 모듈부

270 : 시스템 콜 테이블 데이터베이스

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 리눅스 커널 백도어 탐지 시스템, 이를 이용한 커널 백도어 탐지 방법 및 커널 데이터 복구 방법에 관한 것으로, 특히 리눅스 악성 커널 모듈인 리눅스 커널 백도어를 탐지하고, 이와 같은 커널 백도어에 의해서 조작되거나 변경된 커널 데이터를 감지하여 원래의 정상적인 상태로 복구할 수 있는 리눅스 백도어 탐지 시스템, 이를 이용한 커널 백도어 탐지 방법 및 커널 데이터 복구 방법에 관한 것이다.

일반적으로, 해커(Hacker)에 의해 공격을 당한 리눅스 시스템(Linux System) 내에는 해커에 의해서 어떠한 형태의 백도어(Backdoor) 또는 루트킷(Rootkit)이 설치된다.

이렇게 설치된 백도어는 해커만이 알 수 있는 시스템 상의 치명적인 취약성을 인위적으로 구축하여 시스템에 대한 접속을 용이하게 하거나, 다른 시스템에 대한 공격을 쉽게 수행하는데 이용된다. 한편, 루트킷은 다른 시스템에 침입한 후 다음에 대비하여 백도어나 트로이 목마를 심거나, 침입흔적을 숨기기 위한 도구 모음이다.

이러한, 응용 프로그램 백도어(Application Program Backdoor) 또는 일반적인 루트킷은 프로세스(Process) 및 네트워크(Network) 상태 등과 같이 시스템의 정보를 얻는데 사용되는 프로그램 파일(Program File)을 트로이 버젼으로 변경하는 형태를 취하기 때문에 파일 시스템 무결성 검사와 같은 종래의 탐지 기법을 이용해서 쉽게 발견할 수 있다.

그러나, 커널(Kernel) 기반 루트킷의 일종인 리눅스용 커널 백도어(예: Knark)는 커널 모듈의 형태로 메모리에 적재되기 때문에 사용자 및 응용 프로그램이 커널 백도어의 존재를 확인할 수 있는 방법이 없다. 현재, 응용 프로그램 수준의 백도어와는 달리 커널 백도어를 탐지하고 대응하기 위한 체계적인 방법이 발명되어 있지 않으며, 이와 같은 커널 모듈이 적재되는 것을 방지하기 위한 커널 모듈 관리 도구 또한 존재하지 않는다. 또한, 커널에 적재된 커널 백도어를 탐지하고, 적재 과정에서 변경된 커널 내부의 데이터를 감지하고 복구할 수 있는 기법이 알려져 있지 않고 있다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명은 상기의 문제점을 해결하기 위해 안출된 것으로, 리눅스 커널 백도어와 같은 악성 커널 모듈을 탐지할 수 있는 커널 백도어 탐지 시스템 및 탐지 방법을 제공하는데 그 목적이 있다.

또한, 본 발명은 리눅스 커널 백도어에 의해 변경된 커널 데이터를 정상적인 상태로 복구 시킬 수 있는 커널 데이터 복구 방법을 제공하는데 또 다른 목적이 있다.

이를 위해, 본 발명에서는 커널 공간의 메모리 영역에 적재가 시도되는 리눅스 커널 모듈에 대해서 1차적으로 그 모듈이 적재가 허용되는지를 검사하는 1차 커널 백도어 탐지 과정과, 2차적으로 메모리 영역에 적재되는 커널 모듈이 커널 백도어와 같은 악성 커널 모듈로서 커널 데이터를 변경시키는지를 탐지하는 2차 커널 백도어 탐지 과정과, 변경된 커널 데이터를 다시 정상적인 값으로 복구시키는 복구 과정을 제공한다.

또한, 본 발명의 1차 커널 백도어 탐지 과정에서는 오직 허용된 커널 모듈 만이 메모리 영역에 적재되도록 하기 위해서 커널 내부에 허용 커널 모듈에 대한 목록을 보관하고, 이 목록을 질의하고 갱신하기 위해서 특수한 파라미터를 이용하여 시스템 콜을 호출하며, 리눅스의 'create_module' 시스템 콜을 가로채 커널 모듈이 메모리 영역에 적재되기 전에 그 것이 허용된 커널 모듈인지를 확인하는 방법을 제공한다.

또한, 본 발명의 2차 커널 백도어 탐지 과정에서는 리눅스의 'init_module' 및 'delete_module' 시스템 콜을 가로채는 방법을 통해 적재될 커널 모듈이 커널 내부의 커널 데이터를 변경하는지를 감시하여 그 커널 모듈이 커널 백도어인지를 판별하는 방법을 제공한다.

또한, 본 발명의 복구 과정에서는 커널 백도어에 의해 변경된 커널 데이터인 커널 시스템 콜 테이블, 네트워크 프로토콜 핸들러 및 커널 모듈 목록 정보를 감지하여 이를 원래의 정상적인 값으로 복구시키는 방법을 제공한다.

발명의 구성 및 작용

본 발명은 사용자 영역에 위치되며, 커널 영역 내에 적재가 허용되는 허용 커널 모듈의 목록을 추가, 삭제 및 질의하기 위하여 커널 모듈 관리 프로그램을 내장하는 커널 모듈 관리부와, 상기 커널 모듈 관리부로부터 등록 요청되는 상기 허용 커널 모듈의 목록을 관리하는 허용 커널 모듈 관리부와, 상기 허용 커널 모듈 관리부에 의해 등록 허가된 상기 허용 커널 모듈의 목록을 저장하는 허용 커널 모듈 데이터베이스와, 상기 허용 커널 모듈 데이터베이스에 저장된 상기 허용 커널 모듈의 목록을 토대로 상기 사용자 영역으로부터 적재 요청되는 적재 커널 모듈을 상기 커널 영역 내에 적재하는 커널 모듈 적재 관리부를 포함하는 커널 백도어 탐지 시스템을 제공한다.

또한, 본 발명은 상기 커널 백도어 탐지 시스템을 이용한 커널 백도어 탐지 방법에 있어서, 상기 사용자 영역으로부터 상기 커널 영역으로 허용 커널 모듈의 목록을 등록하는 단계와, 상기 단계에서 등록되는 상기 허용 커널 모듈의 목록을 토대로 상기 사용자 영역으로부터 적재 시도된 적재 커널 모듈에 대한 적재 허용 여부를 탐지하는 단계와, 상기 단계에서 적재가 허용되는 상기 적재 커널 모듈에 의해 상기 커널 영역에 존재하는 커널 데이터가 변경되는지를 탐지하는 단계를 포함하는 커널 백도어 탐지 방법을 제공한다.

또한, 본 발명은 상기 커널 백도어 탐지 시스템을 이용한 커널 데이터 복구 방법에 있어서, 상기 사용자 영역으로부터 상기 커널 영역으로 허용 커널 모듈의 목록을 등록하는 단계와, 상기 단계에서 등록되는 상기 허용 커널 모듈의 목록을 토대로 상기 사용자 영역으로부터 적재 시도된 적재 커널 모듈에 대한 적재 허용 여부를 탐지하는 단계와, 상기 단계에서 적재가 허용되는 상기 적재 커널 모듈의 이름을 상기 커널 원본 데이터베이스의 커널 원본 데이터의 보안 커널 모듈 목록에 추가하는 단계와, 상기 적재 커널 모듈을 상기 커널 영역에 적재하는 단계와, 상기 적재 커널 모듈이 상기 커널 영역에 정상적으로 적재되었는지를 검사하는 단계와, 상기 단계에서 상기 적재 커널 모듈이 정상적으로 적재되었을 경우, 상기 커널 영역에 존재하는 커널 데이터가 변경되었는지 검사하는 단계와, 상기 단계에서 상기 커널 데이터가 변경되었을 경우, 변경된 커널 데이터를 복구하고, 로그값을 저장하는 단계를 포함하는 커널 데이터 복구 방법을 제공한다.

이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 설명하기로 한다. 그러나, 본 발명은 이하에서 개시되는 실시예에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예는 본 발명의 개시가 완전하도록하며 통상의 지식을 가진자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이다.

도 1은 본 발명의 바람직한 실시예에 따른 리눅스 커널 백도어 탐지 시스템의 구성도이다.

도 1을 참조하면, 본 발명의 리눅스 커널 백도어 탐지 시스템은 전체적으로 사용자 영역으로 정의되는 사용자 공간(100)과 커널 영역으로 정의되는 커널 공간(200)으로 분리된다.

사용자 공간(100)은 커널 내에 적재가 허용되는 커널 모듈 목록을 추가, 삭제 및 질의하기 위하여 커널 모듈 관리 프로그램이 내장되는 커널 모듈 관리부(110)를 포함한다. 여기서, 커널 모듈 목록은 현재 커널에 적재되어 있는 커널 모듈을 관리하기 위하여 커널이 사용하고 있는 단일 연결 리스트(Single Linked List) 형태의 커널 데이터이다.

커널 공간(200)은 상기 사용자 공간(100)에 포함된 커널 모듈 관리부(110)를 제외한 모든 기능 모듈부를 포함한다. 예컨대, 허용 커널 모듈 관리부(210), 허용 커널 모듈 데이터베이스(220), 커널 모듈 적재 관리부(230), 커널 데이터 검증/복구 모듈부(240), 커널 원본 데이터베이스(250), 시스템 콜 감시/복구 모듈부(250) 및 시스템 콜 테이블 데이터베이스(270)를 포함한다.

허용 커널 모듈 관리부(210)는 커널에 적재가 허용될 커널 모듈 목록을 관리하는 모듈이다. 허용 커널 모듈 데이터베이스(220)는 커널에 적재가 허용되는 커널 모듈 이름을 포함한 커널 내부의 데이블이 저장되는 데이터베이스(Database)이다. 커널 모듈 적재 관리부(230)는 사용자 공간(100)으로부터 커널 모듈 적재 요청을 받아 처리하는 관리자 모듈이다. 커널 데이터 검증/복구 모듈부(240)는 커널 데이터의 변경 유무를 검증하고 복구하는 모듈이다. 커널 원본 데이터베이스(250)는 변경되기전 정상적인 커널 원본 데이터가 저장되는 데이터베이스이다. 시스템 콜 감시/복구 모듈부(260)는 시스템 콜 테이블(System Call Table)을 실시간으로 감시하고 복구하기 위한 모듈이다. 시스템 콜 테이블 데이터베이스(270)는 커널 내부에 존재하는 시스템 콜 테이블을 저장하는 데이터베이스이다.

상기와 같은 구성을 포함하는 리눅스 커널 백도어 탐지 시스템의 전체 동작 특성을 간략하게 설명하면 다음과 같다.

우선, 사용자 공간(100)의 커널 모듈 관리부(110)는 허용 대상 커널 모듈(Kernel Module)(이하, '허용 커널 모듈'이라 함)들의 이름 목록들을 허용 커널 모듈 데이터베이스(220)에 등록하기 위해 상기 허용 커널 모듈들의 이름 목록들을 포함한 데이터를 허용 커널 모듈 관리부(210)로 전송하여 등록 요청을 한다. 이 때, 커널 모듈 관리부(110)에 의한 허용 커널 모듈 등록 요청은 커널 모듈 관리 프로그램을 실행시킴으로써 이루어진다.

허용 커널 모듈 관리부(210)는 커널 모듈 관리부(110)로부터 전송된 소정 허용 커널 모듈에 대한 등록 요청을 수락 또는 거부할 수 있는데, 그 기준은 허용 커널 모듈의 이름 목록과 동일한 커널 이름이 허용 커널 모듈 데이터베이스(220)에 존재하는지 그 유무에 따라 결정된다.

이 때, 소정 허용 커널 모듈에 대한 커널 모듈 관리부(110)의 등록 요청이 허용 커널 모듈 관리부(210)에 의해 수락되는 경우에만, 허용 커널 모듈 관리부(210)는 상기 허용 커널 모듈의 이름을 단일 연결 리스트 형태로 허용 커널 모듈 데이터베이스(220)에 저장한다.

이와 같이, 단일 연결 리스트 형태로 허용 커널 모듈 데이터베이스(220)에 저장된 다수의 허용 커널 모듈들의 목록들은 적재 커널 입력부(120)를 통해 커널 모듈 적재 관리부(230)로 적재 시도된 커널 모듈(이하, '적재 커널 모듈'이라 함)들의 적재 허용 여부를 판단하는 기준 데이터로 이용된다.

한편, 정상적인 관리자 또는 시스템 침입자에 의해 적재 커널 입력부(120)로부터 입력되는 적재 커널 모듈은 커널 모듈 적재 관리부(230)에 의해 수락되거나 거부될 수 있는데, 이 기준은 상기 허용 커널 모듈의 등록 요청 방법과 같이 적재 커널 모듈의 이름 목록과 동일한 커널 모듈의 이름이 허용 커널 모듈 데이터베이스(220)에 존재하는지 그 유무에 따라 결정된다.

상세히 하면, 커널 모듈 적재 관리부(230)는 적재 커널 입력부(120)로부터 입력되는 적재 커널 모듈이 커널 백도어 또는 악성 커널 모듈인지를 탐지(이하, '1차 커널 백도어 탐지'라 함)하기 위하여 상기 적재 커널 모듈의 이름이 허용 커널 모듈 데이터베이스(220)에 존재하는지를 확인한다.

이 때, 상기 적재 커널 모듈의 이름이 허용 커널 모듈 데이터베이스(220)에 존재하는 경우에만 'create_module' 시스템 콜이 성공적으로 이루어져 'insmod' 프로그램(즉, 적재 커널 모듈을 커널 내에 적재하기 위한 프로그램)으로 복귀할 수 있도록 한다.

그러나, 상기 적재 커널 모듈의 이름이 허용 커널 모듈 데이터베이스(220)에 존재하는 경우에도 상기 적재 커널 모듈이 커널 백도어 또는 악성 커널 모듈일 가능성을 전혀 배제할 수 없다. 만일, 상기 적재 커널 모듈이 커널 백도어 또는 악성 커널 모듈일 경우에는 커널 공간(200)의 메모리 영역(미도시)에 상기 적재 커널 모듈 적재시 커널 내의 시스템 콜 테이블, 네트워크 프로토콜 핸들러(Network Protocol Handler) 및 커널 모듈 목록을 표현하는 데이터(이하, '커널 데이터'라 함)가 변경되는 경우가 발생하게 된다.

이에 따라, 커널 모듈 적재 관리부(230)의 관리자는 상기 적재 커널 모듈의 이름이 허용 커널 모듈 데이터베이스(220)에 존재하여 'create_module' 시스템 콜 이 이루어지면, 'init_module' 및 'delete_module' 시스템 콜 후에 커널 데이터 검증/복구 모듈부(240)를 통해 커널 데이터의 변경 유무를 탐지(이하, '2차 커널 백도어 탐지'라 함)한다.

커널 데이터 검증/복구 모듈부(240)는 커널 원본 데이터베이스(250)에 미리 저장되어 있는 커널 원본 데이터를 이용해서 커널 데이터의 변경 유무를 검사한다. 이 때, 커널 데이터 값이 변경된 경우에는 커널 메모리 영역에 적재된 적재 커널 모듈을 커널 백도어 또는 악성 커널 모듈로 판단하고, 이 변경된 커널 데이터를 원래의 정상적인 상태로 복구한다.

예컨대, 커널 원본 데이터베이스(250)에는 커널 백도어 또는 악성 커널 모듈에 의해서 변경될 가능성이 있는 커널 데이터의 커널 모듈 목록을 복구시키기 위해서 보안 커널 모듈 목록이 저장된다. 여기서, 보안 커널 모듈 목록은 정상적인 커널 모듈 목록과 일치하는 정보를 가지고 있다. 이에 따라, 커널 백도어 또는 악성 커널 커널 모듈에 의해서 커널 모듈 목록이 변경되어 보안 커널 모듈 목록과 동일하지 않게 되면, 이는 악성 커널 모듈에 의해서 커널 모듈 목록이 변경되었다는 것을 나타낸다.

즉, 커널 공간(200)의 메모리 영역에 존재하는 커널 모듈 목록은 단일 연결 리스트를 구조를 하고 있고, 커널 데이터 중에서 'module_list' 변수는 커널 모듈 목록에 존재하는 커널 모듈 중에서 가장 최근에 적재된 커널 모듈 노드(즉, 구성 요소)를 가리키는 주소값을 가지고 있다. 이에 따라, 'create_module' 시스템 콜의 복귀값을 이용하여 상기 주소값이 변경되었는지를 탐지하고, 별도의 보안 커널 모 듈 목록이 변경되었다고 판단되면, 커널 모듈 목록에서 변경된 부분의 노드값을 보안 커널 모듈 목록을 이용하여 복구한다.

또한, 리눅스 커널 백도어 탐지 시스템은 커널 백도어가 커널 내에 적재된 직후가 아닌 다른 시점에서도 커널 타이머(Kernel Timer) 조작을 통해서 커널 데이터가 변경될 수 있으므로, 시스템 콜 감시/복구 모듈부(260)를 통해 시스템 콜 테이블 데이터베이스(270)에 저장된 시스템 콜 테이블의 무결성을 검사하고, 변경된 경우에는 원래의 상태로 복구하는 동작이 수행된다.

이하에서는, 상기에서 설명한 본 발명의 리눅스 커널 백도어 탐지 시스템의 전체 동작 특성을 '등록 과정', '1차 커널 백도어 탐지 과정', '2차 커널 백도어 탐지 과정' 및 '복구 과정'으로 세분화하여 설명하기로 한다.

<등록 과정>

'등록 과정'은 커널 모듈 관리부(110)와 허용 커널 모듈 관리부(210) 사이에서 이루어지는 허용 커널 모듈 등록 과정으로서 도 2에 도시된 흐름도를 참조하여 설명하면 다음과 같다.

도 2를 참조하면, 특정 커널 모듈을 허용 커널 모듈 목록에 등록하기 위하여 커널 모듈 관리부(110)(도 1 참조)의 관리자에 의해 커널 모듈 관리 프로그램을 실행한다(단계 S21).

이어서, 미리 정의된 인자를 이용하여 특정 시스템 콜을 호출한다(단계 S22). 이 단계는 커널 모듈 관리부(110)의 관리자가 등록하고자 하는 허용 커널 모듈의 이름을 커널 공간(200)(도 1 참조)의 허용 커널 모듈 관리부(210)(도 1 참조) 의 관리자에게 전달하기 위하여 특정 시스템 콜을 호출하는 단계이다.

예컨대, 상기 특정 시스템 콜에는 'settimeofday' 표준 유닉스 시스템 콜(이하, 'settimeofday 시스템 콜'이라 함)을 일례로 들 수 있는데, 'settimeofday' 시스템 콜은 두개의 버퍼를 파라미터로 가진다. 따라서, 커널 모듈 관리 프로그램은 'settimeofday' 시스템 콜의 두번째 파라미터에 등록하고자 하는 커널 모듈의 이름을 저장하여 'settimeofday' 시스템 콜을 호출한다.

즉, 'settimeofday' 시스템 콜은 메모리 공간에 대응되게 주소값의 형태를 갖는 두 개의 버퍼를 파라미터로 받아들인다. 이 때, 주소값은 0 내지 10과 같은 범위의 값을 가지지 않는다. 따라서, 첫번째 파라미터의 값으로 0 내지 10 사이의 값을 이용하고, 두 번째 파라미터가 가리키는 메모리 주소 공간에는 등록하고자 하는 허용 커널 모듈의 이름을 저장하여 'settimeofday' 시스템 콜을 호출하는 방법을 취할 수 있다. 이 때, 변형된 'settimeofday' 시스템 콜의 전체적인 동작은 하기와 같은 <가상 코드>(Pseudo-Code)로 표현될 수 있다.

<가상 코드>

```
'if(first_parameter is between 0 and 10){

extract module-name from second_parameter
```

register module-name to allowed_kernel_module_list

} else {

call normal settimeofday system call

}'

상기 단계 S22에서 특정 시스템 콜 호출 동작이 이루어지면 자동적으로 커널 모듈 관리부(110)로부터 허용 커널 모듈 관리부(210)의 관리자에게 허용 커널 모듈이 전달된다(단계 S23).

상기 단계 S23에서 허용 요청된 허용 커널 모듈이 허용 커널 모듈 관리부(210)의 관리자에게 전달되면, 허용 커널 모듈 관리부(210)의 관리자는 커널 모듈 관리부(110)로부터 전송된 해당 커널의 이름이 허용 커널 모듈 데이터베이스(220)(도 1 참조)의 커널 모듈 목록에 존재하는지를 검사한다(단계 S24).

상기 단계 S24에서 해당 커널의 이름이 허용 커널 모듈 데이터베이스(220)의 커널 모듈 목록에 존재할 경우에는 커널 모듈 관리자(110)의 커널 모듈 관리 프로그램을 종료하고, 존재하지 않을 경우에는 허용 커널 모듈 데이터베이스(220)에 단일 연결 리스트 형태로 허용 커널 모듈의 이름 목록을 추가한다(단계 S25).

<1차 커널 백도어 탐지 과정>

'1차 커널 백도어 탐지 과정'은 정상적인 관리자 또는 시스템 침입자에 의해 적재 커널 입력부(120)(도 1 참조)로부터 커널 모듈 적재 관리부(230)(도 1 참조)로 커널 모듈의 적재가 시도될 경우, 이 적재 시도된 적재 커널 모듈이 커널 백도어 또는 악성 커널 모듈인지를 검사하는 과정으로서 도 3에 도시된 흐름도를 통해 설명하면 다음과 같다.

도 3을 참조하면, 정상적인 관리자 또는 시스템 침입자는 적재 커널 모듈을 적재 커널 입력부(120)를 통해 커널 공간(200)의 메모리 영역에 적재하기 위해 'insmod' 프로그램을 실행한다(단계 S31). 여기서, 'insmod'(Insert Module) 프로그램은 커널 모듈을 적재하기 위하여 사용되는 표준 리눅스 프로그램으로서, 정상적인 시스템 관리자에 의해서 실행되거나, 커널의 내부 중요 커널 데이터를 변경시키는 목적을 가진 악성 커널 모듈을 적재하기 위하여 시스템 침입자에 의해서 실행되는 프로그램이다.

상기 단계 S31에서 정상적인 관리자 또는 시스템 침입자에 의해 'insmod' 프로그램이 정상적으로 실행되면, 적재가 시도된 적재 커널 모듈의 이름을 커널 모듈 적재 관리부(230)의 관리자로 전달하기 위하여 'create_module' 시스템 콜 호출 동작이 이루어진다(단계 S32).

상기 단계 S32에서 'create_module' 시스템 콜 호출 동작이 정상적으로 완료되면, 적재 시도된 적재 커널 모듈의 이름이 커널 모듈 적재 관리부(230)의 관리자에게 전달된다(단계 S33).

상기 단계 S33에서 적재 커널 모듈의 이름이 커널 모듈 관리부(230)의 관리자로 전달되면, 커널 모듈 적재 관리부(230)의 관리자는 적재 시도된 적재 커널 모듈의 이름이 허용 커널 모듈 데이터베이스(220)의 커널 모듈 이름 목록에 존재하는지를 검사한다(단계 S34).

상기 단계 S34에서 적재 커널 모듈의 이름이 허용 커널 모듈 데이터베이스(220)의 커널 모듈 이름 목록에 존재할 경우에는 'create_module' 시스템 콜로 정상적으로 복귀한 후(단계 S35), 'init_module' 시스템 콜을 호출하여 적재 커널 모듈을 커널 공간(200)의 메모리 영역에 적재시킨다(단계 S36 및 단계 S37).

상기 단계 S38에서 적재 커널 모듈이 커널 공간(200)의 메모리 영역에 정상적으로 적재가 완료되면, 'init_module' 시스템과 'insmod' 프로그램을 종료하여 '1차 커널 백도어 탐지 과정'을 종료한다(단계 S38 및 단계 S39).

한편, 상기 단계 S34에서 적재 커널 모듈의 이름이 허용 커널 모듈 데이터베이스(220)의 커널 모듈 이름 목록에 존재하지 않을 경우에는 바로 단계 S39로 이동하여 'insmod' 프로그램을 종료한다.

<2차 커널 백도어 탐지 과정>

'2차 커널 백도어 탐지 과정'은 커널 공간(200)의 메모리 영역에 미리 저장된 커널 데이터가 상기 '1차 커널 백도어 탐지 과정'에서 이루어지는 적재 커널의 적재 과정시 데이터 변경이 있는지를 검사하는 과정으로서, 도 4에 도시된 흐름도를 통해 설명하면 다음과 같다.

도 4를 참조하면, 우선 '2차 커널 백도어 탐지 과정'은 '1차 커널 백도어 탐지 과정'에서 도 3에 도시된 단계 S34 후에 이루어지는 과정으로서 하기에서 설명되는 단계 S41 및 단계 S42는 단계 S35 및 단계 S36과 동일한 과정으로 볼 수 있다.

상기 단계 S41는 'create_module' 시스템 콜을 복귀하기 위한 복귀값을 저장하는 단계로서, 별도의 변수에 복귀값을 복사하는 과정이다. 여기서, 복귀값은 적재 커널이 적재될 커널 공간(200)의 메모리 영역을 가리키는 주소값(Address)이며, 이 값은 실제로 도 3에서 설명한 'create_module' 시스템 콜이 호출되고, 종료되었 을 때 자동적으로 커널 공간(200)의 메모리 영역에 저장된다.

상기 단계 S42는 'init_module' 시스템 콜을 호출하여 'init_module' 시스템을 실행하는 단계이다. 이 단계에서 'init_module' 시스템 콜 호출이 정상적으로 이루어지면, 커널 데이터 검증/복구 모듈부(240)(도 1 참조)에서는 커널 원본 데이터베이스(250)(도 1 참조)에 저장된 커널 원본 데이터를 이용하여 커널 데이터가 변경되었는지를 검사한다(단계 S43).

상기 커널 원본 데이터는 커널 백도어 또는 악성 커널 모듈이 커널 내부의 커널 데이터를 변경시키더라도 항상 정상적인 값으로 유지되는 데이터로서, 그 대상으로는 커널 데이터와 동일하게 시스템 콜 테이블, 커널 모듈 목록 및 프로토콜 핸들러가 있으며, 각각 해당하는 커널 원본 데이터 내의 참조 데이터를 가지고 있다.

상기 단계 S43에서 커널 데이터가 변경되었을 경우, 커널 데이터 검증/복구 모듈부(240)에서는 커널 원본 데이터베이스(250)에 저장된 커널 원본 데이터의 보안 커널 모듈 목록을 이용하여 변경된 커널 데이터를 복구하고, 그 로그값을 저장한다(단계 S44). 상기 로그값은 커널 데이터가 변경된 시점에서 저장되는 로그로서, 커널 데이터의 변경을 발생시킨 커널 모듈의 이름, 상기 커널 모듈을 적재되려고 시도된 시간 및 변경된 커널 데이터의 종류를 포함한다.

한편, 상기 단계 S43에서 커널 데이터가 변경되지 않았을 경우, 단계 S45로 이동하여 '1차 커널 백도어 탐지 과정'을 통과한 적재 커널 모듈을 커널 공간(200)의 메모리 영역에 저장한다(단계 S45).

상기 단계 S44에서 커널 데이터 복구 과정이 완료되면, 단계 S45로 이동하여 '1차 커널 백도어 탐지 과정'을 통과한 적재 커널 모듈을 커널 공간(200)의 메모리 영역에 저장한다.

상기 단계 S45에서 적재 커널 모듈의 적재가 완료되면, 'insmod' 프로그램을 종료한다(단계 S46).

<복구 과정>

'복구 과정'은 커널 원본 데이터 베이스(250)에 저장된 보안 커널 모듈 목록을 이용하여 커널 백도어 또는 악성 커널 모듈에 의해서 커널 데이터가 변경된 것을 감지하고, 변경된 커널 데이터를 복구하는 과정으로서 도 5에 도시된 흐름도를 참조하여 설명하면 다음과 같다.

도 5를 참조하면, 이 도면은 도 4에 도시된 흐름도를 더욱 구체화하여 도시한 도면으로서, '2차 커널 백도어 탐지 과정'과 '복구 과정'을 하나의 흐름도 내에 도시한 흐름도이다.

단계 S51 및 단계 S52는 '1차 커널 백도어 탐지 과정' 및 '2차 커널 백도어 탐지 과정'에서 이루어지는 단계로서, 'insmod' 프로그램이 실행되면 자동적으로 'create_module' 시스템 콜이 호출되어 메모리 할당이 이루어진 후 'create_module' 시스템 콜의 복귀값이 저장되는 단계이다.

상기 단계 S52에서 'create_module' 시스템 콜 복귀값이 저장되면, 본 발명에서 새롭게 제시한 'init_module' 시스템 콜 호출동작을 통해 'init_module' 시스템(이하, 'init_module_new 시스템'이라 함)을 실행한다(단계 S53).

상기 단계 S53에서 'init_module_new' 시스템이 실행되면, 현재 적재 커널 모듈의 이름을 커널 원본 데이터베이스(250)의 커널 원본 데이터에 포함된 보안 커널 모듈 목록에 추가한다(단계 S54).

상기 단계 S54에서 적재 커널 모듈이 보안 커널 모듈 목록에 추가되면, 일반적인 'init_module' 시스템 콜 호출 동작을 통해 현재 적재 커널 모듈을 커널 공간(200)의 메모리 영역에 적재한 후 'init_module' 시스템을 종료한다(단계 S55 내지 단계 S57). 이 과정은 도 3에 도시된 단계 S36 내지 단계 S38과 동일한 과정으로 이루어진다.

상기 단계 S57에서 'init_module' 시스템이 종료되면, 'init_module' 시스템의 복귀값을 검사하여 적재 커널 모듈이 커널 공간(200)의 메모리 영역에 정상적으로 적재되었는지를 검사한다(단계 S58). 예컨대, 'init_module' 시스템의 복귀값을 검사하여 복귀값이 '-1'이면, 적재 커널 모듈이 적재되지 않음을 의미하고, 복귀값이 '-1'이 아니면, 정상적으로 적재 커널 모듈이 적재된 것을 의미한다.

상기 단계 S58에서 적재 커널 모듈이 커널 공간(200)의 메모리 영역에 정상적으로 적재되지 않았을 경우에는 보안 커널 모듈 목록에 추가된 적재 커널 모듈의 이름을 삭제한 후(단계 S59), 단계 S60으로 이동한다.

상기 단계 S58에서 적재 커널 모듈이 커널 공간(200)의 메모리 영역에 정상적으로 적재되었을 경우에는 단계 S60으로 이동하여 커널 내부의 커널 모듈 목록이 변경되었는지를 검사한다.

상기 단계 S60에서 커널 내부의 커널 모듈 목록이 변경되었을 경우에는 단계 S61로 이동하여 변경된 커널 모듈 목록를 복구하고, 그 로그값을 저장한 후 단계 S62로 이동한다.

한편, 상기 단계 S60에서 커널 내부의 커널 모듈 목록이 변경되지 않았을 경우에는 단계 S61로 이동하여 'init_module_new' 시스템을 종료한 후, 'insmod' 프로그램을 종료한다.

상기에서 설명한 본 발명의 기술적 사상은 바람직한 실시예에서 구체적으로 기술되었으나, 상기한 실시예는 그 설명을 위한 것이며 그 제한을 위한 것이 아님을 주의하여야 한다. 또한, 본 발명은 본 발명의 기술 분야의 통상의 전문가라면 본 발명의 기술적 사상의 범위 내에서 다양한 실시예가 가능함을 이해할 수 있을 것이다.

발명의 효과

상술한 바와 같이, 본 발명은 '1차 커널 백도어 탐지 과정' 및 '2차 커널 백도어 탐지 과정'과 같이 2단계의 커널 백도어 탐지 과정을 통해 리눅스 시스템 내에 커널 백도어와 같은 악성 커널 모듈이 설치되는 것을 효과적으로 탐지할 수 있다.

또한, 본 발명은 커널 백도와 같은 악성 커널 모듈에 의해 변경된 커널 데이터를 '2차 커널 백도어 탐지 과정'을 통해 탐지하고, 변경된 커널 데이터를 정상적인 커널 데이터로 복구시킴으로써 커널 백도어에 의한 침입을 효과적으로 방지할 수 있다.

(57) 청구의 범위

청구항 1.
사용자 영역에 위치되며, 커널 영역 내에 적재가 허용되는 허용 커널 모듈의 목록을 추가, 삭제 및 질의하기 위하여 커널 모듈 관리 프로그램을 내장하는 커널 모듈 관리부;

상기 커널 모듈 관리부로부터 등록 요청되는 상기 허용 커널 모듈의 목록을 관리하는 허용 커널 모듈 관리부;

상기 허용 커널 모듈 관리부에 의해 등록 허가된 상기 허용 커널 모듈의 목록을 저장하는 허용 커널 모듈 데이터베이스; 및

상기 허용 커널 모듈 데이터베이스에 저장된 상기 허용 커널 모듈의 목록을 토대로 상기 사용자 영역으로부터 적재 요청되는 적재 커널 모듈을 상기 커널 영역 내에 적재하는 커널 모듈 적재 관리부를 포함하는 것을 특징으로 하는 커널 백도어 탐지 시스템.

청구항 2.
제 1 항에 있어서, 상기 허용 커널 모듈 관리부는 상기 커널 모듈 관리부로부터 등록 요청된 상기 허용 커널 모듈의 목록이 상기 허용 커널 모듈 데이터베이스에 존재하지 않을 경우에만 등록 요청을 수락하는 것을 특징으로 하는 커널 백도어 탐지 시스템.

청구항 3.
제 1 항에 있어서, 상기 허용 커널 모듈의 목록은 상기 허용 커널 모듈 데이 터베이스에 단일 연결 리스트 형태로 저장되는 것을 특징으로 하는 커널 백도어 탐지 시스템.

청구항 4.
제 1 항에 있어서, 상기 커널 영역 내에 위치되며, 상기 허용 커널 모듈에 대한 커널 원본 데이터를 저장하는 커널 원본 데이터베이스; 및

상기 커널 원본 데이터베이스에 저장되는 상기 커널 원본 데이터를 토대로 상기 커널 영역에 저장되는 커널 데이터의

변경 유무를 검증하고, 복구하는 커널 데이터 검증/복구 모듈부를 더 포함하는 것을 특징으로 하는 커널 백도어 탐지 시스템.

청구항 5.
제 4 항에 있어서, 상기 커널 원본 데이터 및 커널 데이터는 시스템 콜 테이블, 네트워크 프로토콜 핸들러 및 커널 모듈 목록을 포함하는 데이터인 것을 특징으로 하는 커널 백도어 탐지 시스템.

청구항 6.
제 1 항에 있어서, 상기 커널 영역 내에 위치되며, 상기 커널 내에 저장되는 커널 데이터의 시스템 콜 테이블을 저장하는 시스템 콜 테이블 데이터베이스; 및

상기 커널 데이터의 변경 유무를 탐지하기 위하여 상기 시스템 콜 테이블의 무결성을 검사하고, 복구하는 시스템 콜 감시/복구 모듈부를 더 포함하는 것을 특징으로 하는 커널 백도어 탐지 시스템.

청구항 7.
제 1 항 내지 제 6 항중 어느 하나의 항의 구성을 가지는 커널 백도어 탐지 시스템을 이용한 커널 백도어 탐지 방법에 있어서,

(a) 상기 사용자 영역으로부터 상기 커널 영역으로 허용 커널 모듈의 목록을 등록하는 단계;

(b) 상기 (a)단계에서 등록되는 상기 허용 커널 모듈의 목록을 토대로 상기 사용자 영역으로부터 적재 시도된 적재 커널 모듈에 대한 적재 허용 여부를 탐지하는 단계; 및

(c) 상기 (b)단계에서 적재가 허용되는 상기 적재 커널 모듈에 의해 상기 커널 영역에 존재하는 커널 데이터가 변경되는지를 탐지하는 단계를 포함하는 것을 특징으로 하는 커널 백도어 탐지 방법.

청구항 8.
제 7 항에 있어서, 상기 (a)단계는,

(a-1) 상기 사용자 영역의 커널 모듈 관리부를 통해 상기 커널 영역의 허용 커널 모듈 관리부로 상기 허용 커널 모듈의 이름을 전달하는 단계;

(a-2) 상기 커널 모듈 관리부로부터 전달된 상기 허용 커널 모듈의 이름이 상기 허용 커널 모듈 데이터베이스에 저장된 허용 커널 모듈 목록에 존재하는지를 검사하는 단계; 및

(a-3) 상기 (a-2) 단계에서 상기 허용 커널 모듈의 이름이 존재하지 않을 경우, 상기 허용 커널 모듈의 이름을 상기 허용 커널 모듈 목록에 등록하는 단계를 포함하는 것을 특징으로 하는 커널 백도어 탐지 방법.

청구항 9.
제 8 항에 있어서, 상기 (a-1) 단계는

(a-1-1) 상기 허용 커널 모듈의 이름을 등록하기 위하여 상기 사용자 영역의 커널 모듈 관리부의 커널 모듈 관리 프로그램을 실행하는 단계;

(a-1-2) 상기 허용 커널 모듈의 이름을 상기 커널 영역의 허용 커널 모듈 관리부로 전달하기 위하여 특정 시스템 콜을 호출하는 단계; 및

(a-1-3) 상기 커널 모듈 관리부로부터 상기 허용 커널 모듈 관리부로 상기 허용 커널 모듈의 이름을 전달하는 단계를 포함하는 것을 특징으로 하는 커널 백도어 탐지 방법.

청구항 10.
제 9 항에 있어서, 상기 특정 시스템 콜은 메모리 영역에 대응되게 주소값의 형태를 가지는 두 개의 버퍼를 파라미터로 가지며, 첫 번째 버퍼의 파라미터 값으로는 0 내지 10 사이의 값을 이용하고, 두 번째 버퍼의 파라미터가 가리키는 메모리 영역에는 상기 허용 커널 모듈의 이름을 저장하여 호출되는 것을 특징으로 하는 커널 백도어 탐지 방법.

청구항 11.
제 8 항에 있어서, 상기 (a-3)단계에서 상기 허용 커널 모듈의 이름은 단일 연결 리스트 형태로 상기 허용 커널 모듈

목록에 등록되는 것을 특징으로 하는 커널 백도어 탐지 방법.

청구항 12.
제 7 항에 있어서, 상기 (b)단계는,

(b-1) 상기 사용자 영역으로부터 상기 커널 영역의 커널 모듈 적재 관리부로 적재 커널 모듈의 이름을 전달하는 단계;

(b-2) 상기 사용자 영역으로부터 전달된 상기 적재 커널 모듈의 이름이 상기 허용 커널 모듈 데이터베이스에 저장된 허용 커널 모듈 목록에 존재하는지를 검사하는 단계; 및

(b-3) 상기 (b-2) 단계에서 상기 적재 커널 모듈의 이름이 존재하는 경우, 상기 적재 커널 모듈을 상기 커널 영역에 적재하는 단계를 포함하는 것을 특징으로 하는 커널 백도어 탐지 방법.

청구항 13.
제 12 항에 있어서, 상기 (b-1)단계는,

(b-1-1) 상기 사용자 영역의 'insmod' 프로그램을 실행하는 단계; 및

(b-1-2) 상기 적재 커널 모듈의 이름을 상기 커널 모듈 적재 관리부로 전달하기 위하여 'create_module' 시스템 콜을 호출하는 단계를 포함하는 것을 특징으로 하는 커널 백도어 탐지 방법.

청구항 14.
제 12 항에 있어서, 상기 (b-3)단계는,

(b-3-1) 상기 (b-2)단계에서 상기 적재 커널 모듈의 이름이 존재하는 경우, 상기 'create_module' 시스템 콜로 복귀하는 단계;

(b-3-2) 상기 적재 커널 모듈을 상기 커널 영역에 적재하기 위하여 'init_module' 시스템 콜을 호출하는 단계; 및

(b-3-3) 상기 'init_module' 시스템과, 'insmod' 프로그램을 순차적으로 종료하는 단계를 포함하는 것을 특징으로 하는 커널 백도어 탐지 방법.

청구항 15.
제 7 항에 있어서, 상기 (c)단계는,

(c-1) 상기 (b)단계에서 상기 적재 커널 모듈 적재시, 상기 커널 영역에 존재하는 커널 데이터가 변경되는 것을 감지하기 위하여 상기 커널 데이터와 커널 원본 데이터베이스에 저장된 커널 원본 데이터를 비교하는 단계를 포함하는 것을 특징으로 하는 커널 백도어 탐지 방법.

청구항 16.
제 15 항에 있어서, 상기 (c-1)단계는,

(c-1-1) 상기 적재 커널 모듈을 적재하기 위하여 'create_module' 시스템 콜의 복귀값을 복사하는 단계; 및

(c-1-2) 상기 커널 데이터와 상기 커널 원본 데이터를 비교하기 위하여 'init_module' 시스템 콜을 호출하는 단계를 포함하는 것을 특징으로 하는 커널 백도어 탐지 방법.

청구항 17.
제 16 항에 있어서, 상기 복귀값은 상기 적재 커널 모듈이 적재될 상기 커널 영역을 가리키는 주소값이며, 이 값은 상기 'create_module' 시스템 콜이 호출되고, 종료되었을 때 자동적으로 상기 커널 영역에 저장되는 것을 특징으로 하는 커 널 백도어 탐지 방법.

청구항 18.
제 4 항 내지 제 6 항중 어느 하나의 항의 구성을 가지는 커널 백도어 탐지 시스템을 이용한 커널 데이터 복구 방법에 있어서,

(a) 상기 사용자 영역으로부터 상기 커널 영역으로 허용 커널 모듈의 목록을 등록하는 단계;

(b) 상기 (a)단계에서 등록되는 상기 허용 커널 모듈의 목록을 토대로 상기 사용자 영역으로부터 적재 시도된 적재 커널 모듈에 대한 적재 허용 여부를 탐지하는 단계;

(c) 상기 (b)단계에서 적재가 허용되는 상기 적재 커널 모듈의 이름을 상기 커널 원본 데이터베이스의 커널 원본 데이터의 보안 커널 모듈 목록에 추가하는 단계;

(d) 상기 적재 커널 모듈을 상기 커널 영역에 적재하는 단계;

(e) 상기 적재 커널 모듈이 상기 커널 영역에 정상적으로 적재되었는지를 검사하는 단계;

(f) 상기 (e)단계에서 상기 적재 커널 모듈이 정상적으로 적재되었을 경우, 상기 커널 영역에 존재하는 커널 데이터가 변경되었는지 검사하는 단계; 및

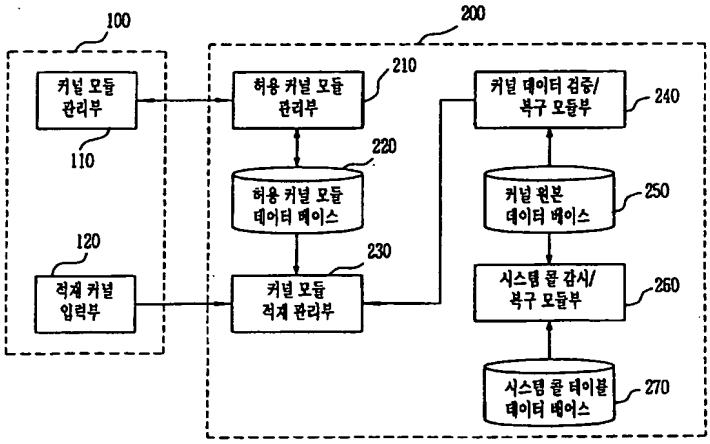
(g) 상기 (f)단계에서 상기 커널 데이터가 변경되었을 경우, 변경된 커널 데이터를 복구하고, 로그값을 저장하는 단계를 포함하는 것을 특징으로 하는 커널 데이터 복구 방법.

청구항 19.

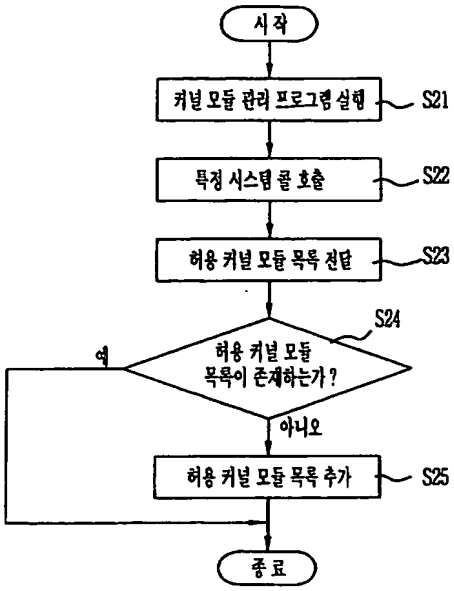
제 18 항에 있어서, 상기 (e)단계에서 상기 적재 커널 모듈이 정상적으로 적재되지 않았을 경우, 상기 (c)단계에서 추가된 상기 적재 커널 모듈의 이름을 삭제하는 단계를 더 포함하는 것을 특징으로 하는 커널 데이터 복구 방법.

도면

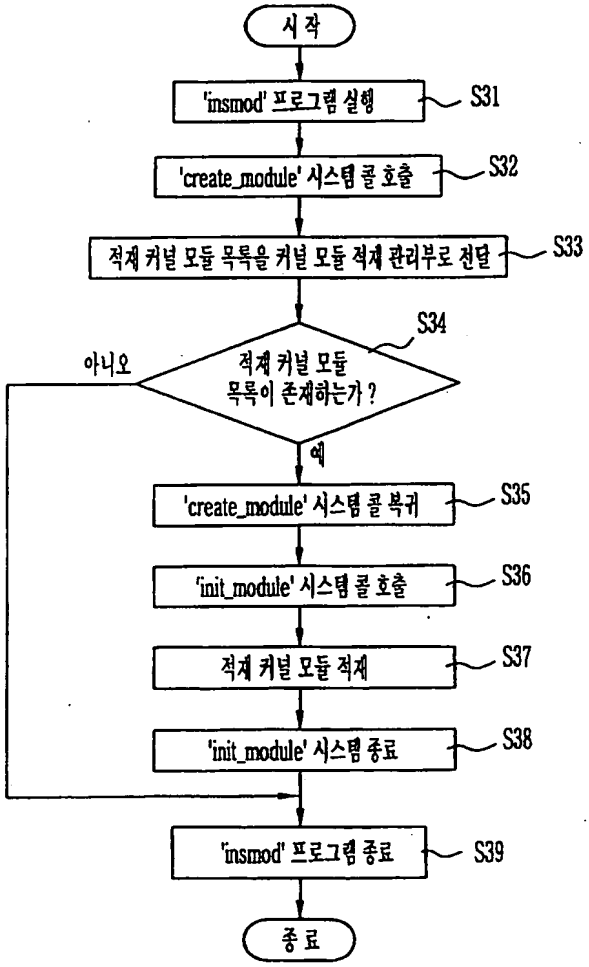
도면1



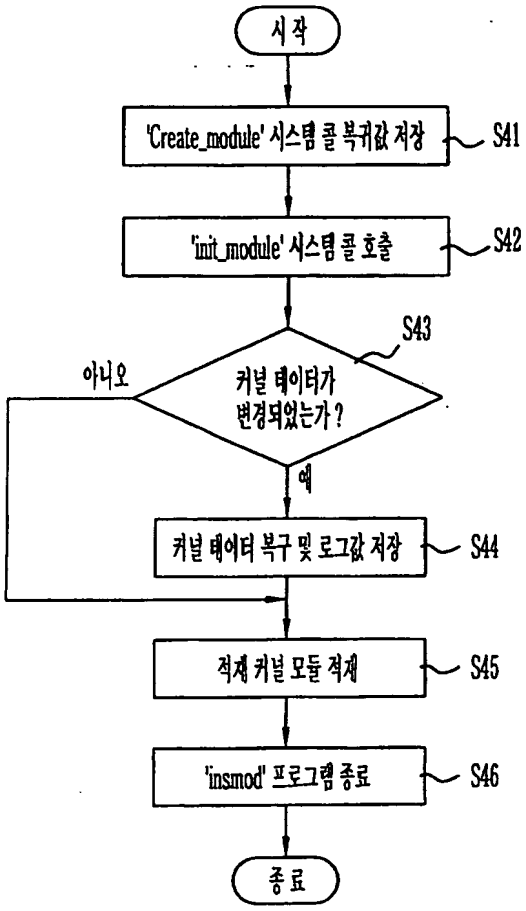
도면2


시작
커널 모듈 관리 프로그램 실행
S21
특정 시스템 콜 호출
S22
허용 커널 모듈 목록 전달
S23
S24
허용 커널 모듈
목록이 존재하는가?
예
아니오
허용 커널 모듈 목록 추가
S25
종료

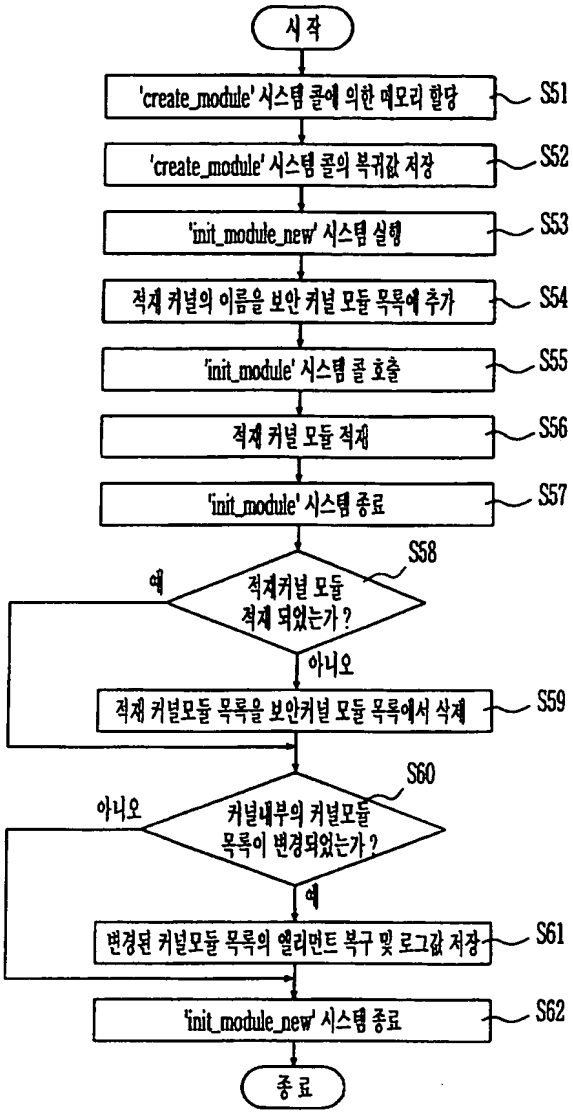
도면3


시작
'insmod' 프로그램 실행
S31
'create_module' 시스템 콜 호출
S32
적재 커널 모듈 목록을 커널 모듈 적재 관리부로 전달
S33
S34
적재 커널 모듈
목록이 존재하는가?
아니오
예
'create_module' 시스템 콜 복귀
S35
'init_module' 시스템 콜 호출
S36
적재 커널 모듈 적재
S37
'init_module' 시스템 종료
S38
'insmod' 프로그램 종료
S39
종료

도면4


시작
'Create_module' 시스템 콜 복귀값 저장
S41
'init_module' 시스템 콜 호출
S42
S43
아니오
커널 데이터가
변경되었는가?
예
커널 데이터 복구 및 로그값 저장
S44
적재 커널 모듈 적재
S45
'insmod' 프로그램 종료
S46
종료

도면5


시작
'create_module' 시스템 콜에 의한 메모리 할당
S51
'create_module' 시스템 콜의 복귀값 저장
S52
'init_module_new' 시스템 실행
S53
적재 커널의 이름을 보안 커널 모듈 목록에 추가
S54
'init_module' 시스템 콜 호출
S55
적재 커널 모듈 적재
S56
'init_module' 시스템 종료
S57
S58
적재커널 모듈 적재 되었는가 ?
예
아니오
적재 커널모듈 목록을 보안커널 모듈 목록에서 삭제
S59
S60
커널내부의 커널모듈 목록이 변경되었는가 ?
아니오
예
변경된 커널모듈 목록의 엘리먼트 복구 및 로그값 저장
S61
'init_module_new' 시스템 종료
S62
종료